

## **Appendix 1 – List of Relevant Policies**

- **Capital Planning and Investment Control (CPIC) Policy:**  
<http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/2120.pdf>
- **Capital Planning and Investment Control (CPIC) Procedures for the Office of Management and Budget (OMB) Exhibit 300:**  
<http://intranet.epa.gov/cpic/fy2008/cpic-procedures-sept05.pdf>
- **Data Exchange and Collection Procedure:**  
[http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/CIO\\_2122-P-04.0.pdf](http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/CIO_2122-P-04.0.pdf)
- **Data Standards Policy:**  
<http://intranet.epa.gov/oeiintra/imitpolicy/qic/ciopolicy/2133.0.pdf>
- **Enterprise Architecture Policy:**  
<http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO-2122.1.pdf>
- **EPA System Life Cycle Management (SLCM) Policy:**  
[http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO\\_2121.1.pdf](http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO_2121.1.pdf)
- **EPA System Life Cycle Management (SLCM) Requirements Guidance:**  
[http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO\\_2121-G-01.0.pdf](http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO_2121-G-01.0.pdf)
- **EPA Information Security Policy:**  
<http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO-2150-3.pdf>
- **System Life Cycle Management (SLCM) Procedure--Mobile App Concept Approval Process**  
[http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO\\_2121-P-03.0.pdf](http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO_2121-P-03.0.pdf)  
(See APPENDIX E of the System Life Cycle Management Procedure)
- **Privacy Policy:**  
<http://intranet.epa.gov/oei/imitpolicy/qic/pdfs/cio2151.0.pdf>
- **Procedures for Preparing and Publishing Privacy Act System of Records Notices:**  
<http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO2151-P-03.1.pdf>
- **The following standards and guidance are applicable to the Federal Risk and Authorization Management Program (FedRAMP)**  
(<http://www.gsa.gov/portal/category/102371>):
  - A NIST Definition of Cloud Computing [NIST SP 800-145]
  - Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
  - Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
  - Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]

- General Criteria for the Operation of Various Types of Bodies Performing Inspection [International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17020:1998]
- Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
- Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
- Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60, Revision 1]
- Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
- Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
- Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 3]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30]
- Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

